Windows 10 versus iOS 10

A Lab-Based Feature Comparison of Windows 10 and iOS 10 in Security and Manageability Categories

PIQUE SOLUTIONS

December 2016

MICROSOFT SPONSORED THE DEVELOPMENT OF THIS WHITE PAPER. THE UNDERLYING LAB-BASED TESTING, RESEARCH AND ANALYSIS WERE EXECUTED INDEPENDENTLY BY PIQUE SOLUTIONS.

Contents

Executive Summary 3

Testing Methodology 4

Key Findings 6

Identity and Authorization 8

- Authentication 8
- Biometric Support 9
- Testing Scores 9

Information Protection 10

- Protected Storage (DAR) 10
- Protected Communication (DIT) 11
- Data Protection in Progress (DIU) 12
- Testing Scores 14

Threat Resistance 14

- Device Integrity 14
- Application Protection 15
- Testing Scores 17

Management and Reporting 17

- Device Enrollment 17
- Device Configuration 19
- App Management 20
- Remote Administration 20
- Diagnostics and Monitoring 21
- Testing Scores 22

Conclusions 22

Executive Summary

Where the goal of cyber prevention has been to reduce the probability of an attack against the organization, cyber resilience looks to reduce the impact of these attacks through risk management. A cyber resilience program still considers detection and prevention techniques, but it also assumes that a breach is likely. This stance emphasizes anticipation, agility and adaptation.

The first objective of cyber resilience is to align security with assets. The security stack should protect the business against the threats specifically relevant to those business assets. Often, security is misaligned with no awareness by the business due to a lack of data on which to base a decision. A growing number of technologies and architectural practices exist to improve resilience in the face of cyber threats, however, these improvements come with costs as well as benefits.

Pique Solutions conducted a lab-based comparative analysis of the resilience capabilities of Microsoft's Windows 10 and Apple's iOS 10. The analysis assessed the level of assurance those capabilities provided an organization, the utility of those capabilities, and the impact on the user experience.

With Windows 10 and Windows 10 Mobile, Microsoft has unified the PC, tablet, and phone operating systems into a single OS. Windows 10 and Windows 10 Mobile are co-developed, share the same core and the same app model, and access the same app store. The variation in OS is associated with the version of Windows 10; for this white paper, we looked at Windows 10 Pro, Windows 10 Enterprise, Windows 10 Mobile, and Windows 10 Mobile Enterprise. In some cases, the underlying chipset provides extra functionality, such as virtualization support on x86 processors, or the OS version has specific features related to its core function, such as telephony on Windows 10 Mobile. Otherwise, security, management, and apps built on the Universal Windows Platform are the same across PCs, tablets, and mobile devices. This paper will refer to the operating system as Windows 10, with variances and differences noted where applicable.

Measured against the key criteria for this analysis—security assurance and usability — Pique Solutions maintains that Windows 10 provides a higher level of security assurance with a lower impact on usability. Windows 10 provides cost-effective two-factor authentication for phones, tablets, and PCs and eliminates the user password, mitigating the risk of compromise due to lost or stolen credentials and providing ease of use. Windows 10 protects enterprise data in a way that is transparent to the user, including the ability for a user to share a single app for both personal and work tasks. Windows 10 provides conditional access to enterprise resources based on device health attestation. Windows 10 leverages a unified OS architecture and app development platform across device types to streamline provisioning of devices and apps, including distribution of critical security updates and patches.

iOS 10 provides incremental improvements over previous versions of iOS for the enterprise environment. While iOS 10 does provide a strong level of assurance by implementing a hardware based trusted chain of boot and strict controls over app management, it still requires third-party integration for two-factor authentication and, when compared to Windows 10, has a greater impact on usability when managing and protecting enterprise data.

Within the current cyber landscape where targeted persistent attacks by well-funded adversaries are a reality, organizations need to consider to what extent their architecture achieves cyber resiliency objectives, or how effectively it incorporates cyber resiliency techniques. Windows 10 can deliver resilient devices that meet the most stringent security and enterprise management requirements, while providing those controls in such a way that is transparent to the end user and enhances rather than impedes productivity.

Testing Methodology

The overall testing methodology developed by Pique Solutions was as follows:

1. Determine the security characteristics and capabilities required to mitigate the risks of device access to enterprise resources, including the ability to store, transmit, and use enterprise data.
2. Build an environment to simulate a lightweight enterprise architecture, including common components present in most organizations such as directory services.
3. Select mobile devices and management systems that provide the assessment of Windows 10 Mobile, Windows 10 Mobile Enterprise, Windows 10, Windows 10 Pro, Windows 10 Enterprise, and iOS 10.
4. Manually confirm how selected devices perform defined tasks in the testing framework.
5. Publish a detailed assessment of the findings.

To assess Windows 10 and iOS 10 using industry-accepted standards and definitions, Pique Solutions referenced the security characteristics and required capabilities founded in the principles identified in Special Publication (SP) 1800-4b of the National Institute of Standards and Technology (NIST) Cybersecurity Practice Guide. The NIST analyzed the content and concepts from multiple standards to generate the necessary security characteristics, including findings documented in NIST SP 800-124, NIST SP 800-164, the National Security Agency (NSA) mobile capabilities package, and the appropriate National Information Assurance Partnership (NIAP) protection profiles. Pique Solutions revised and updated the NIST characteristics where it deemed appropriate to address missing functionality, to correlate security characteristics with vendor-described capabilities, and to improve the overall presentation and flow of the paper.

To organize the presentation, we grouped the capabilities into four areas.

Identity and Authorization

- Authentication: Local authentication of user to device and apps, remote authentication of user, remote authentication of device
- Trust Model: Implementation of user and device roles for authentication, credential and token storage and use
- Biometric Support: Methods, store, use

Information Protection

- Protected Storage (DAR): Device encryption, trusted key storage, hardware security modules
- Protected Communication (DIT): Virtual private network (VPN), per-app VPN
- Data Protection in Progress (DIU): Protected execution environments, data management, data sharing, encrypted memory

Threat Resistance

- Device Integrity: Boot/app/OS/policy verification, trusted integrity reports
- Application Protection: Memory isolation, trusted execution, browser protection

Device/App Management

- Device Enrollment: Discovery, certificate, provisioning
- Device Configuration and Policies Supported: Network, device resources, geo-fencing

- App Management: Delivery, update, configuration, app black/whitelisting
- Remote Administration: Asset management, OS and security updates, lost device, remote wipe
- Diagnostics/Monitoring: Anomalous behavior detection, compliance, root detection

For the testing environment, we used the most widely adopted and common software in the enterprise world: Microsoft Windows Server, Microsoft Active Directory, Office 365 (documents and email), “Enterprise App” (a lightweight limited-functionality app to simulate an enterprise-provided app), “Personal App” (a lightweight limited-functionality app to simulate a personal app), and OneDrive.

The MDM systems used were Microsoft Intune, integrated with the set of Microsoft tools and MobileIron.

The devices used were the following:

1. Lumia 950—Windows 10 Mobile
2. Surface Pro 3—Windows 10 Enterprise
3. iPhone 6s—iOS 10
4. iPad Mini 4—iOS 10

The enterprise mobility specialists configured the test environment and devices, executed all defined scenarios, and published this comparative analysis. Pique Solutions leveraged MDM vendors expressly for real world testing of OS management capabilities. For example, Microsoft Intune offers app wrapping for iOS 10. While a strong capability for data protection, it would require comparative analysis against other vendor-supplied app-wrapping capabilities. For the purpose of parity, Pique Solutions chose MobileIron as an independent MDM provider widely adopted in organizations. Analysis of MDM is beyond the scope and intent of this research project.

To assess OS resilience, we analyzed security and management capabilities against security assurance levels (SALs), a concept introduced in ISA-99.01.01 as described below.

> *Security levels provide a qualitative approach to addressing security for a zone. As a qualitative method, security level definition has applicability for comparing and managing the security of zones within an organization. As more data becomes available and the mathematical representations of risk, threats, and security incidents are developed, this concept will move to a quantitative approach for selection and verification of Security Levels (SL). It will have applicability to both end user companies, and vendors of IACS and security products. It will be used to select IACS devices and countermeasures to be used within a zone and to identify and compare security of zones in different organizations across industry segments.*

ISA99 qualitatively defines four SALs:

- SAL1 – protection against casual or coincidental violation
- SAL2 – protection against intentional violation using simple means
- SAL3 – protection against intentional violation using sophisticated means
- SAL4 – protection against intentional violation using sophisticated means with extended resources

For scoring, SAL’s are assigned numerical values and weighted on utility of capabilities to organizational security. Utility defines whether a capability provides features an organization needs. The total score reflects an overall OS resilience level, or how well an OS would survive an attack and to what level. Pique also evaluated the impact security had on usability. Metrics are time-to-task, error rate, and user satisfaction. Information security always fails to human error when it provides a poor user experience.

Key Findings

Based on Pique Solutions' lab-based comparative feature assessment of Windows 10 and iOS 10 in the security and manageability categories, Windows 10 provides a higher level of security assurance than iOS 10 with a lower impact on usability. The following are the key findings that led us to that conclusion:

Identity and Authorization

- Windows 10 two-factor device authentication provides the same level of security assurance as a smart card token based implementation but with no additional infrastructure cost
- iOS 10 device authentication uses a single factor
- Windows 10 biometrics are a replacement for passwords with a positive impact on both usability security assurances
- iOS Touch ID is an alternative to passwords for user convenience, not a replacement; the password still exists
- Windows 10 is the first enterprise operating system to implement FIDO 2.0 providing the highest level of security assurance for authentication available today; FIDO 2.0 incorporates multifactor authentication with asymmetrical keys and hardware-based attestation

Information Protection

- Windows Information Protection (WIP) manages business data transparently with no impact to usability incurred from secure containers and app wrapping
- iOS 10 provides controls to limit sharing of enterprise data with personal apps, but it does not address device level file sharing (AirDrop is configured separately as a hardware control).

Threat Resistance

- Windows 10 Measured Boot uses hardware to measure the system boot process for integrity
- iOS 10 has hardware root-of-trust laid down during chip fabrication that is implicitly trusted.
- Windows 10 furthers memory protection with control flow integrity, Control Flow Guard (CFG), to combat memory corruption vulnerabilities

Management

- Windows 10 uses Azure Ad integration for single step domain authentication, provisioning, and management
- Windows 10 remote health attestation ensures device compliance from hardware to software; Conditional access limits exposure to devices that are not
- iOS 10 does not provide similar remote health attestation which is limits its jailbreak detection capabilities
- Microsoft has maintained a highly consistent security patch update schedule to address vulnerabilities in a timely manner; patch management is a critical process for organizational security

Testing Scores

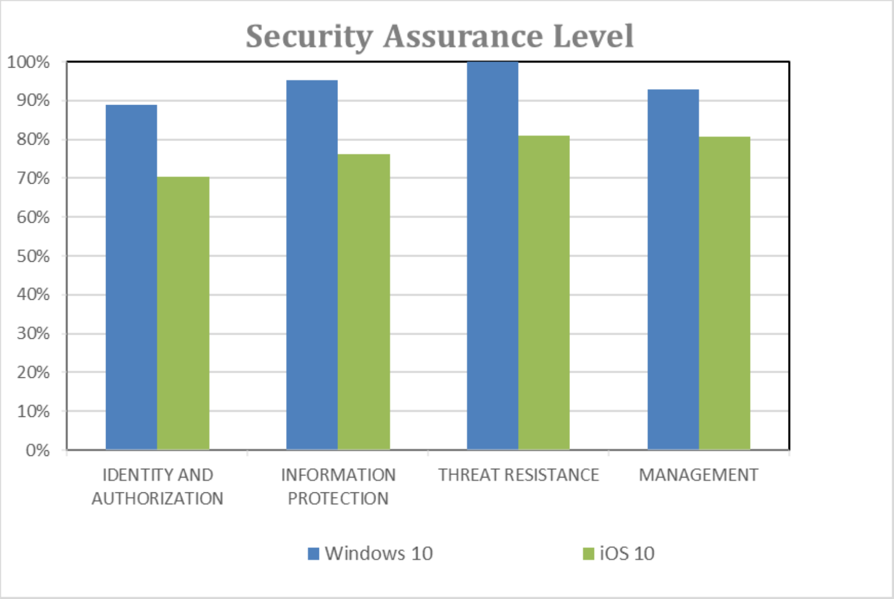

Chart 1. Windows 10 vs. iOS 10 *Security Assurance* Lab-Testing Scores

Overall, Windows 10 consistently scored higher than iOS 10 in every measured category, particularly in identity management, where Windows 10 can provide a unified authentication experience to the user and the enterprise. For data protection, Windows 10 applies encryption and controls to the data in such a way that proves to be both more effective and transparent to the user experience. For threat resistance, Windows 10 adds new capabilities for memory protection not yet seen in an iOS, which again are completely transparent to the user. For management capabilities, Windows 10 offers a diverse range of methods for managing the OS and a streamlined device provisioning and configuration process using domain accounts. Windows 10 also provides conditional access to devices based on remote health attestation.

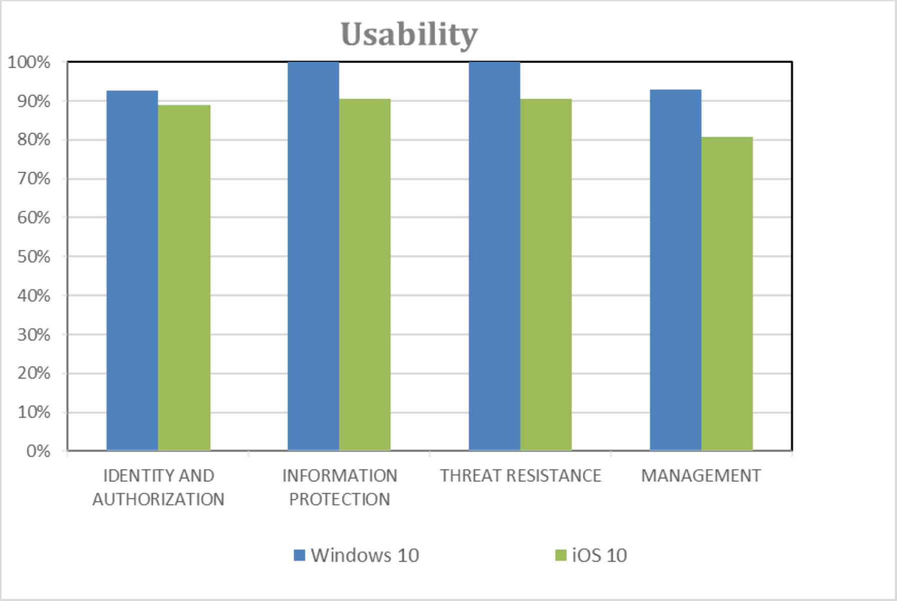

Chart 2. Windows 10 vs. iOS 10 *Usability* Lab-Testing Scores

Identity and Authorization

Identify and Access Management (IAM) provides all the right resources to those users who need them when they need them. The enterprise needs IAM capabilities that address agility in managing distributed systems where users maintain access across multiple device types. IAM should ensure the integrity and authenticity of each user's identity while considering costs of the IAM infrastructure. More importantly, IAM must maintain user simplicity balanced with strong authentication controls.

The most common form of identity is user name and password. Most users need to remember on average at least three passwords, limiting the desire or ability of most people to remember highly complex passwords. Those passwords can be compromised in a matter of minutes, if not seconds, using modern computers. Simply knowing a user's credentials allows another individual to impersonate that identity. Mobile devices, once considered simple low risk personal devices, standardized on a less complex 4-digit PIN for convenience reasons, reducing the complexity factor significantly. Yet, while not strong, password and PIN persist, as they are relatively convenient, easy to implement, and personal to a user. As part of a multi-factor authentication strategy, the password and PIN have the potential to be effective and convenient. Even better, by leveraging biometrics, user identity becomes unique, more personal, and more convenient to the user and the enterprise.

Authentication

Windows 10 provides two-factor authentication for remote enterprise domain authentication of user to device and apps. Windows Hello technology replaces passwords with the combination of a specific device and a biometric gesture or PIN. Windows Hello supports Microsoft accounts, Active Directory (AD), Azure Active Directory, or a non-Microsoft service that supports Fast ID Online (FIDO) 2.0 authentication. Windows 10 is the first OS to utilize FIDO 2.0 in an enterprise environment, and it is a major step forward. FIDO 2.0 supports multifactor authentication with asymmetrical keys in conjunction with hardware-based attestation to confirm the legitimacy of the keys.

After an initial two-step verification during enrollment, the user sets up Windows Hello on a device and then sets a gesture to verify identity, which can be a biometric or a PIN. The Trusted Platform Module (TPM) chip generates authentication keys on the device that are bound to the device. This enables the device as a form of identity in relation to an enterprise domain account. Asymmetric key cryptography authenticates users before granting them access to enterprise apps or online corporate resources. This is similar to methods that power certificate-based authentication with smart cards or that allow cell phones to verify networks but without the need for additional hardware. Windows 10 does not require a personal Microsoft account on devices joined to Azure AD or an on-premises Active Directory domain.

Windows 10 Enterprise protects the authentication system even further by running it in a limited-access virtual container called Credential Guard. Access tokens and tickets are all stored there, fully randomized and managed, with full-length hashes to avoid brute-force attacks.

Apple provides two-factor authentication with iOS 10, but it is specific for Apple ID. This is not enterprise-level two-factor authentication. With Apple ID two-factor authentication, when a user enters his or her Apple ID and password for the first time on a new device, Apple asks the user to verify identity with a 6-digit verification code, presented from another supported device or phone number. An authenticated user does not authenticate on that device again except at a specified time-out period or if he or she erases the device or needs to change the password. This is a decent first step, but it is an opt-in process that the user does not necessarily understand or use. This authentication does not eliminate the password, which is still the primary means of authentication.

iOS 10 requires the implementation of third-party apps for enterprise-domain two-factor authentication of iOS apps. This still does not address enterprise-domain two-factor authentication for the device. iOS 10 does support authentication to enterprise networks through certificate-based single sign-on (SSO). Safari supports SSO for third-party apps that use standard iOS networking APIs. Third-party apps provide two-factor authentication, but this is still a password-based two-factor system.

Biometric Support

Windows Hello is an extensible framework that enables the use of biometric sign-in options for Windows 10. The user's unique biometric identifier enables authenticated access to the device. While currently Windows Hello supports fingerprints, facial recognition, and iris scanning, new hardware may expand currently supported biometrics.

Windows 10 integrates biometrics with the other security components of the device. The user's biometric data used with Windows Hello does not travel across the user's devices and is not centrally stored in the cloud. Windows 10 converts the biometric image taken by the sensor into an algorithmic form and destroys the original image rendering it irretrievable. The algorithmic form of the image is then stored on the TPM that is required on every Windows 10 Mobile device. Not storing biometric images eliminates the risk of using those images to gain illicit access to corporate resources from another device. Built-in anti-spoofing and liveness detection prevents the use of simulated biometrics, such as a photograph of the user's eye, to access a device.

Touch ID is Apple's biometric fingerprint authentication technology. With it, touching the Home button unlocks an iOS 10 device and authorizes purchases on the iTunes Store. App store-distributed apps also have the ability to integrate Touch ID for authentication. A capacitive ring activates the scanner on contact, which then takes a high-resolution picture of a fingerprint. iOS 10 converts that fingerprint into a mathematical formula, encrypts it, and carries it over a hardware channel to the secure enclave on the Apple hardware chipset.

Concerning the app store, only upon successful determination of authentication status, opt-out to password, or canceling out altogether can an app regain control. iOS 10 does not back up ACL-protected items and does not synchronize them between devices. Developers never gain access to user fingerprint data in their apps. More importantly, TouchID is a convenience feature that provides an alternative form of device access where a password is still able to bypass fingerprint authentication.

Testing Scores

Identity	Security Assurance Level (SAL)	Usability
Windows 10	**89**	**93**
iOS 10	**70**	**89**

Windows 10 two-factor device authentication provides the same level of security assurance as a smart card token-based implementation but with no additional infrastructure cost. The two factors could be the device and the user. Moreover, this two-factor authentication is not limited to the OS but provides support for apps and websites. From a security standpoint, this means that an attacker would need to have a user's physical device and the user's biometric information. Because user biometric data is not stored anywhere in Windows 10, the attacker would need the user as well. From a usability perspective, this means the user has nothing to remember while eliminating typical management overhead of resetting user passwords. It also could be a potential costs savings

While both Windows 10 and iOS 10 point toward a unified platform for providing system wide biometric authentication, Windows 10 shows a clear lead in biometrics by providing a framework supporting multiple methods of authentication as well as eliminating the password altogether. iOS 10 currently only has support for fingerprint, which is an alternative to using a PIN, but not a replacement.

Information Protection

As defined with data loss prevention, data controls relate to three functional groupings that correspond to the data lifecycle. These are data at rest (DAR), for data stored on device and other forms of media; data in transit (DIT), for data shared between users and the associated methods of information sharing; and data in use (DIU), for the creation and manipulation of data on the device residing in apps, documents, and system memory. In any data protection strategy, controls would be located as close to the data as possible. The most effective method for data protection is to implement controls on the data, followed by apps serving as data custodians, and lastly on the device and network. Controls may exist at all of the preceding locations for complete management of the data lifecycle.

Protected Storage (DAR)

Encryption is the primary means used to ensure a lost, stolen, or misused device does not lead to the loss or compromise of sensitive information. The cryptographic keys used for encryption should be stored in protected locations in software, firmware, or hardware, with hardware providing the highest level of protection. Tamper-resistant hardware is also preferred for performing cryptographic operations.

Windows 10 implements BitLocker for whole-disk encryption, including OS and data storage partitions. It applies encryption automatically when policy requires it or the user enables it in the Windows settings. Windows 10 accelerates encryption through processor extensions to avoid compromising device performance. The default encryption algorithm on Windows 10 Mobile is 128-bit AES and is configurable as enabled through system management. Windows 10 Enterprise supports 128-bit and 256-bit XTS-AES to provide additional protection from a class of attacks on encryption that rely on manipulating cipher text to cause predictable changes in plain text.

iOS 10 uses a 256-bit device-unique secret key stored in the phone's hardware and does not store these values elsewhere. No software or hardware can read this key. The device-unique key combines with the passcode to generate a passcode key to secure data on the device. The intent is that an attacker cannot remotely extract the device-unique key from the device.

A per-file key encrypts the content of a file, wraps it with a class key, and stores it in the file's metadata, encrypted with the file system key. The hardware key protects the class key and, for some classes, the user's passcode. iOS 10 extends this functionality to more items, including messages, pictures, contacts, and phone call history.

Exhaustive key search techniques on a key space of 128 bits, using the latest streamlining processes, require resources (MIPS, memory, power, and time) many orders of magnitude beyond current capabilities. Any unseen breakthroughs would most certainly apply to 256-bit as well as 128-bit.

Leveraging 256-bit does not necessarily mean better but may lead to a negative impact on system resources and utilization for processing of key algorithms.

Protected Communication (DIT)

The objective of controls for DIT is the ability for the user to establish a protected connection between the device and trusted enterprise resources or with enterprise apps, usually through VPNs. The value of a VPN is that it encrypts a device's Internet connection to provide secure remote enterprise access. However, the use of VPNs does have a slight impact on network performance but with modern networks this may be imperceptible. VPN access also unnecessarily exposes an organization to other apps on a device. VPN access should be granular with the ability to limit access to specific apps.

Windows 10 comes with a VPN platform that includes two types of VPN connections:

- INBOX Protocols
  - IKEv2, PPTP, and L2TP (with L2TP both PSK and Certificate)–based VPNs are supported
  - Inbox VPN uses EAP for authentication. The supported EAP methods are:
    - MSCHAPV2
    - TLS (uses certificate-based authentication including Hello for Work, virtual smart cards, and certificates)
    - TTLS (Outer Method)
      - With the following inner methods:
        - PAP/Chap/MSCHAP/SCHAPv2
        - EAP MSCHAPv2
        - EAP TLS
    - PEAP
      - With the following inner methods:
        - EAP MSCHAPv2
        - EAP TLS

- VPN Plugin Platform for TLS/SSL
  - The VPN plugin platform allows third-party developers to write downloadable VPN apps from the store. The apps currently in the store are Pulse Secure, Cisco, SonicWall, Check Point, MobileIron, and F5; a number of others are coming in the latter half of 2016.

Windows 10 supports a number of OnDemand and Enforcement methods to simplify and secure the VPN connection. Always On enables the VPN to connect automatically when the user turns on his or her phone or if there is a network change. LockDown VPN further enforces policy by only allowing network traffic over the VPN tunnel. App-triggered VPN allows for automatically triggered connections when an app launches. Traffic Filters offer enterprises the ability to manage per-app behavior so that only traffic originating from an approved list of apps flows across the VPN. As another layer, Traffic Filters also provide traffic filtering based on host destination attributes. Rules can include both app-based and traffic-based.

iOS 10 devices work with VPN servers that support the following protocols and authentication methods:

- IKEv2: Support for both IPv4 and IPv6 and the following:
  - Authentication methods: Shared secret, certificates, EAP-TLS and EAP-MSCHAPv2

    - Suite B cryptography: ECDSA certificates, ESP encryption with GCM, and ECP Groups for the Diffie-Hellman Group
    - Additional features: MOBIKE, IKE fragmentation, server redirect, split tunnel
- L2TP over IPSec: User authentication by MS-CHAP v2 password, two-factor token, certificate, machine authentication by shared secret or certificate
- SSL VPN: User authentication by password, two-factor token, and certificates using a third-party VPN client
- Cisco IPSec: User authentication by password, two-factor token, and machine authentication by shared secret and certificates
- PPTP: User authentication by MS-CHAP v2 password, certificate, and two-factor token
- Pulse Secure, Cisco, Aruba Networks, SonicWALL, Check Point, Palo Alto Networks, Open VPN, AirWatch, MobileIron, NetMotion Wireless, and F5 Networks SSL-VPN using the appropriate client app from the App Store.

iOS 10 supports VPN On Demand for networks that use certificate-based authentication defined through profile configuration. iOS 10 also supports Per App VPN, facilitating VPN connections on a much more granular basis. MDM can specify a connection for each managed app and/or specific domains in Safari. iOS 10 supports Always-on VPN, which can be configured for devices managed via MDM and supervised using Apple Configurator or the Device Enrollment Program. Always-on VPN tunnels all IP traffic back to the organization. The default tunneling protocol, IKEv2, secures traffic transmission with data encryption.

Data Protection in Progress (DIU)

The goal of data protection in progress is to limit the sharing of enterprise data with personal apps and services to prevent data loss. This can be accomplished in several ways, including data encryption, app management, and secure containers. Of the three methods, data encryption incurs the lowest impact on system resources and usability. Secure containers and segregated apps incur a higher impact on system resources and on usability. In addition to methods for managing enterprise data within the app, data residing in memory needs to execute only in a protected memory space.

Windows 10 Windows Information Protection (WIP) implements the most effective method for data protection. Because it is integrated into the OS, WIP does not require the implementation of secure container or duplicate apps. WIP encrypts data dynamically based on defined organization policies. By focusing on managing enterprise data regardless of app, WIP provides the enterprise visibility and control of enterprise data without altering the personal user experience. WIP is able to classify data and apps as personal or work to determine which apps have access to business data. This classification also determines what data to encrypt and how users can share that data. AppLocker, a part of the configuration service used by MDM to specify which apps are allowed and/or disallowed, manages app classification sans app wrapping or app modification with an SDK. This means admins do not need to add or remove any classified app from a device, including when wiping enterprise information. WIP does not tamper with existing personal apps and data.

Trusted apps are those designated for corporate use that can access protected work data as well as personal data. Apps that are not part of the trusted app list will not be able to access corporate information stored on the device or on a corporate share. That data remains encrypted when saved to an untrusted location like a USB drive or personal cloud storage account. Furthermore, the keys are under organizational control, so when a user leaves the organization the key is revoked, and the user can no longer decrypt that data regardless of its location or remotely access organizational resources. A key feature of WIP is the ability for Windows 10 apps designed to work on personal and business data in parallel (e.g., People [Contacts], Outlook) while still providing the necessary controls and encryption to work data. For example, documents in Microsoft Word for work could be limited from copy and paste while allowing sharing of personal documents.

WIP allows IT to set four levels of protections for devices accessing corporate resources:

- **Block:** WIP looks for inappropriate data sharing and stops the user from completing the action.
- **Override:** WIP looks for inappropriate data sharing and alerts the user when he or she does something in violation of policy. This protection level lets users override the policy and share the data anyway, but it logs the action to an audit log.
- **Silent:** WIP runs silently, encrypting data and logging when users do something inappropriate, but it does not prompt users or block their actions.
- **Off:** WIP is not active and does not protect data on the device.

Organizations can choose to either block unapproved data sharing (e.g., copying and pasting) outright or allow auditable sharing. With auditable sharing, users can override the WIP-defined restrictions, but if a user attempts unauthorized data sharing, an alert provides the user a warning and an EMM system will log their action. The user can then proceed or cancel the action. When users create new documents, they can manually change the classification from a corporate classification to a personal classification within any allowed app. When a user classifies a new document as personal, the user will not be able to copy and paste information from a corporate document into that new personal document. Classification events are logged for review.

Microsoft Rights Management (RMS), bundled with Office 365, can extend WIP's capabilities. RMS controls, such as authorized print and document and email forwarding controls, augment WIP's app control and copy-and-paste control. These controls extend to other operating systems, including iOS 10, in addition to Windows 10.

iOS 10 limits the sharing of enterprise data using managed apps. Managed apps can include free, paid, and enterprise apps. Managed apps have the following restrictions and capabilities:

- Managed Open In
    - Allow documents from unmanaged sources in managed destinations. Enforcing this restriction prevents personal sources and accounts from opening documents in managed destinations.
    - Allow documents from managed sources in unmanaged destinations. Enforcing this restriction prevents managed sources and accounts from opening documents in personal destinations.
- App developers can identify configuration settings that can be set or after app installation as a managed app.
- App developers can identify app settings that can be read using MDM.
- Prevent managed apps from backing up data to iCloud or iTunes.
- Downloads from Safari are considered managed documents if they originate from a managed domain.
- Prevent managed apps from storing data in iCloud.

If a preferred app for personal use is considered managed, the user is required to find alternate means of managing personal documents. If the user has a current app that is unmanaged, such as Adobe Acrobat Reader DC, the enterprise will reclassify the app as a managed app and will no longer support unapproved data. This requirement creates redundancy in the associated apps for opening attachments, a common operation on mobile devices. iOS 10 also provides a restriction that prevents managed apps from backing up data to iCloud or iTunes, preventing recovery of managed app data if the user reinstalls the apps.

Testing Scores

Information Protection	Security Assurance Level (SAL)	Usability
Windows 10	**95**	**100**
iOS 10	**76**	**90**

When comparing Windows 10 device encryption with iOS 10, they are equivalent, including the use of hardware-based key storage. Both platforms are strong in this area. We also did not observe any particular advantages or disadvantages with VPN communication implemented in Windows 10 or iOS 10. This is strong for both platforms.

While both Windows 10 and iOS 10 provide comparable strong levels of encryption, we consider Windows 10 to be the superior implementation given the granular ability for encryption at the data level versus iOS 10's approach of applying encryption to the app. This is part of Windows 10's ability to provide data protection at the data level using WIP. WIP's level of integration within the OS and enterprise apps also leads to a less intrusive user experience, where iOS 10 requires an app be designated personal or work with no dual-use capabilities.

Threat Resistance

It is unrealistic to consider any system is free from all defects and secure from all external threats. Attackers exploit vulnerabilities to infect devices with malware through two methods: program errors or intended features. Program errors introduce methods by which an attacker can introduce an exploit to the system by circumventing access controls to allow for remote access. These exploits subsequently use this error to download and execute other malware, propagating on the system and across the network. Intended features allow for unintended use, such as browsers that allow execution of code on the local operating system, introducing a method by which viruses, worms, and other threats can obtain remote access to a system.

To reduce the impact of data loss and malware propagation on a compromised system, the OS needs to be resilient and designed in a manner that prevents new or unknown apps from gaining unreasonably broad or complete access to files stored in memory or in apps running on the device.

Device Integrity

Windows 10 devices utilize the Unified Extensible Firmware Interface with Secure Boot to validate the integrity of the device, firmware, and bootloader using cryptographically validated digital signatures. This process establishes an essential root in a chain of trust that extends from the device hardware and firmware to the OS. After the OS loader starts, Trusted Boot verifies that the remaining Windows boot related components are trustworthy and have integrity. The Windows kernel, in turn, verifies every other component of the Windows startup process including the boot drivers and startup files. Trusted Boot will detect any file modifications and attempt to restore those files to a known valid configuration before starting Windows. Trusted Boot requires Microsoft signs all code in the operating system, including OEM drivers and the antivirus solution, thereby providing the next layer integrity validation. Windows Store or a trusted enterprise store must digitally sign all Windows 10 apps.

Microsoft extends the primary integrity validation process by including a second hardware-backed process called Measured Boot. This uses TPM hardware to baseline the boot process for critical startup-related components, including firmware, Windows boot components, and drivers. TPM provides isolation and protection of the baseline data against tampering attacks. Windows 10 can leverage this baseline data along with additional security and configuration criteria for Conditional Access scenarios which will leverage the Windows Device Health Attestation (DHA) cloud-based service as a means to remotely attest that the device truly has integrity. From here management systems using the DHA service may grant or deny the device access to resources based on this check. This is particularly important in detecting rooted devices that may be able to circumvent less sophisticated integrity controls.

On iOS 10, a secure boot chain also validates the integrity of the device, firmware, and bootloader. At the initial power on, the device application processor executes code from read-only memory known as the Boot ROM. This is the hardware root of trust, laid down during chip fabrication, and is implicitly trusted. The Boot ROM code contains the Apple Root CA public key used to verify Apple has signed the Low-Level Bootloader (LLB) before allowing it to load. Each subsequent step ensures that Apple also signs the next layer of the boot process. When the LLB finishes its tasks, it verifies and runs the next-stage bootloader, iBoot, which in turn verifies and runs the iOS kernel.

Once the iOS 10 kernel has started, it controls which user processes and apps run. To ensure that all apps come from a known and approved source and have not been tampered with, iOS requires that all executable code be signed using an Apple-issued certificate; Apple signs default apps. An Apple-issued certificate also signs and validates third-party apps. Mandatory code signing extends integrity validation from the OS to apps, and prevents third-party apps from loading unsigned code resources or using self-modifying code. Apple allows the enterprise to define a list of managed and unmanaged apps on a device to define what apps run based on enterprise approval.

Application Protection

Windows 10 apps and even portions of the OS itself run inside their own isolated sandbox called an AppContainer. The security policy of a specific AppContainer defines the operating system capabilities that apps have access to, from within the AppContainer. A capability is a Windows 10 device resource such as geographical location information, a camera, a microphone, networking, and sensors. Apps are isolated from one another and can communicate only by using predefined communications channels and data types.

Many exploits and malware attacks need to know where specific processes or system functions reside in memory. Address Space Layout Randomization (ASLR) randomly arranges the memory addresses of executable code, system libraries, and related programming constructs to reduce the likelihood of exploits knowing where code and data are located. Microsoft has improved the ASLR implementation in Windows 10 over previous versions by multiplying the complexity of memory space prediction. Leveraging TPM, ASLR memory randomization becomes unique across devices limiting the effectiveness of successful exploits across multiple systems. ASLR is available for apps while Windows 10 applies ASLR holistically across the OS to help mitigate the risks of sandbox escapes.

Windows 10 implements Data Execution Prevention (DEP) to refuse to execute any code located in user-writable areas of memory, protected random heap memory allocations and memory-management algorithms. This collection of technologies further reduces the likelihood that vulnerabilities can enable successful exploits. To counter these defense mechanisms, attackers leverage code that is already available on the system using return-oriented programming. Windows 10 is the first OS to implement a method for locking down enforcing an app's flow of control once loaded into memory, dubbed Control Flow Guard (CFG). This vulnerability mitigation technique helps prevent return-oriented programming attacks and is a critical capability for browsers; Microsoft Edge has CFG enabled. These groupings of technologies represent Microsoft's decades of experience combatting malware on Windows platforms, which have been the most used OS's in the enterprise and by the consumer.

Microsoft Edge uses AppContainer-based sandboxing to help protect the system against vulnerabilities. Microsoft Edge does not run legacy binary extensions, including Microsoft ActiveX, Java, Silverlight, and Browser Helper Objects, which significantly reduces risk. SmartScreen provides anti-phishing URL filtering, checks downloads using Application Reputation, and can even help prevent drive-by exploits. If SmartScreen detects malicious content on a site, it can block the site itself or, in some cases, just specific content on the site.

In iOS 10, all third-party apps run in an app sandbox so they are restricted from accessing files stored by other apps or from making changes to the device. This prevents apps from gathering or modifying information stored by other apps. If a third-party app needs to access information other than its own, it does so only by using services explicitly provided by iOS 10. Users' apps are segregated from system files and resources. The majority of iOS runs as the non-privileged user "mobile," as do all third-party apps. The entire OS partition mounts as read-only. APIs do not allow apps to escalate their own privileges or to modify other apps or iOS 10 itself.

Safari, along with all iOS built-in apps, uses ASLR to ensure randomization of memory regions upon launch. iOS 10 splits the virtual memory into two regions—one writable and one executable—and keeps the location of those regions hidden. Randomly arranging the memory addresses of executable code, system libraries, and related programming constructs reduces the likelihood of many sophisticated exploits. iOS 10 uses ARM's Execute Never (XN) feature that marks memory pages as non-executable, a form of DEP. Only apps under tightly controlled conditions use memory pages marked as both writable and executable: The kernel checks for the presence of the Apple-only dynamic code-signing entitlement. Safari uses this functionality for its JavaScript JIT compiler. In iOS 9, Apple launched a feature known as Kernel Patch Protection, wherein a low-level function periodically checks the integrity of the operating system kernel. In iOS 10, Apple further hardened KPP against known attacks, making exploitation more difficult.

Testing Scores

Threat Resistance	Security Assurance Level (SAL)	Usability
Windows 10	100	100
iOS 10	81	90

Windows 10 provides two distinct threat resistance features over iOS Windows 10 Measured Boot uses hardware to measure the system boot process for integrity. iOS 10 has hardware root-of-trust laid down during chip fabrication that is implicitly trusted and does provide very strong integrity validation from the hardware to apps, but it does not allow for remote attestation of conditions to define criteria such as not allowing unencrypting of the drive on a jailbroken device. The second feature is Windows 10 improvement on memory protection with control flow integrity, called Control Flow Guard (CFG), intended to combat memory corruption vulnerabilities.

Management and Reporting

Every organization has its specific needs and device policies, but these needs tend to fit one of three scenarios:

1. Organizations that allow users to personalize their devices because the users own the devices or because the organization's policy does not require stringent controls.
2. Organizations that do not allow users to personalize their devices or they limit personalization, because the organization owns the devices and security considerations are paramount.
3. Organizations that support a combination of personal and corporate-issued devices, requiring a mix of policies addressing both scenarios.

In every scenario, organizations need device management. The intent of device management is to optimize the functionality and security of a mobile communications network while minimizing cost and downtime. Device management provides four key capabilities: visibility, device configuration, app management, and operational support. Device management provides awareness of mobile devices requesting access to corporate resources. It allows the business to understand who owns what devices and what apps are present on them. Device management allows an admin to configure and maintain devices with access to corporate resources in accordance with corporate policies. Device management provides distribution and maintenance of enterprise-approved apps, including protection through app policy enforcement. Finally, device management provides the ability to remotely manage and support a device with specific actions, as supported by the mobile operating system manufacturer. This ensures that a mobile device maintains the latest updates, that users can access their device in an emergency and that a lost or stolen device is not a liability to the organization.

Device Enrollment

The current versions of management tools manage all device types running Windows 10. Existing enterprise management tools, such as Group Policy, Windows Management Instrumentation, PowerShell scripts, Orchestrator runbooks, and System Center tools, will continue to work for Windows 10 on PCs. Devices running Windows 10 also include a built-in agent for MDM to enroll and manage devices. MDM vendors use the Microsoft MDM protocol for communication with a Windows 10 device, which supports Open Mobile Alliance's Device Management Protocol 1.2.1. The MDM client allows MDM to configure policy settings, deploy apps and updates, and perform other management tasks. MDM sends configuration requests and collects inventory through the MDM client.

MDM uses the Apple Push Notification Service (APNS) to maintain persistent communication with Apple iOS devices across both public and private networks. MDM requires multiple certificates, including an APNS certificate to talk to devices, an SSL certificate to communicate securely, and a certificate to sign configuration profiles. Organizations are required to renew APNS certificates annually. When a certificate expires, an MDM solution cannot communicate with Apple devices until the organization updates its certificate.

Table 1. EMM Vendor Support: Windows 10 vs. iOS 10

	Windows 10	iOS 10
BlackBerry	√	√
Citrix	√	√
Google		√
IBM MaaS 360	√	√
Lightspeed Systems	√	√
Matrix 42	√	√
Microsoft Intune	√	√
MobileIron	√	√
SAP	√	√
Soti	√	√
Symantec	√	√
VMWare AirWatch	√	√

Windows 10 personal-owned devices use a Microsoft Work Account, which acts as a secondary account on the device specific to enterprise management and resource access. Corporate-owned devices join the enterprise using domain accounts as the primary device authentication. Azure AD integration allows for single sign-on to native applications including Mail, Word, OneDrive and Azure AD web apps Azure AD Join also provides single sign-on for on-premise resources and authentication for Windows Store for Business. An administrator creates and applies the provisioning package before delivery of a device to the user, or the user can apply the provisioning package during initial configuration.

iOS 10 devices are designated as supervised or personal. Devices can be set up as supervised only prior to activation (before Setup Assistant first appears on a new or fully erased device). Apple Deployment Programs automatically enrolls supervised devices in MDM during initial setup. On personal devices, in most cases, users decide whether to enroll, and they can disassociate their devices from the management server at any time. Personal devices can have profiles removed if the user knows the passcode, even if the option is set to Never in the general settings. To enforce participation, the enterprise will need to consider creative requirements that enforce MDM by limiting enterprise resources, such as enterprise Wi-Fi network access, but this is not the same as the health attestation present in Windows 10.

iOS 10 supports provisioning packages for MDM, with distribution available via email attachment or web page publishing. iOS 10 support for MDM also includes cryptographic signing and encryption of provisioning packages with password-based user access. MDM can set up mail and other user accounts automatically. MDM can also prepopulate the account payloads with a user's name, email address, certificate identities for authentication, and signing. iOS 10 devices typically use Simple Certificate Enrollment Protocol to create unique identity certificates for authenticating an organization's services. However, to achieve the same benefits as Windows 10 single step MDM enrollment, iOS 10 enrollment requires a multistep process including use of the Microsoft Azure Authenticator App for Azure AD and a third-party client for MDM.

Device Configuration

Using the built-in Windows 10 MDM client, Windows 10 allows for MDM-managed restrictions for several features, as listed below. These capabilities are exposed to any compatible MDM system.

- Mandate device passcodes and specify requirements.
- Enforce internal storage encryption.
- Enable or disable SD card use.
- Disable developer unlock.
- Allow VPN over mobile data or data roaming.
- Configure and distribute ActiveSync settings.
- Permit the use of Wi-Fi and Wi-Fi Sense hotspot auto-connect.
- Configure different types of certificates such as root, CA, and publisher certificates.
- Restrict camera, Cortana, location data, telemetry, Bluetooth, Internet sharing, or adding non-Microsoft accounts.
- Prohibit the use of location information in Search.
- Deny Microsoft account connection authentication.
- Disallow Sync My Settings across multiple devices.
- Restrict non-Windows Store apps.
- Locate devices and review breadcrumb history.
- Selectively or fully wipe lost, stolen, or noncompliant devices.
- Restrict manual device decommissioning.

iOS 10 supports non-removable MDM profiles for supervised devices to lock the device to MDM so users cannot bypass management or unenroll them. In the latest release, Apple added more enterprise features, including integration with enterprise mobility management (EMM) systems, to enforce and override activation locks on the devices and force the device to report its location if it is being actively managed. Several device management features are only available on supervised devices or have other specific requirements, as shown below in the management tasks available in iOS 10.

- Enable/allow/remove activation Lock.
- Enable/disable diagnostics and usage reporting: **Available only with Shared iPad.**
- Clear passcode.
- Clear restrictions password: **Available for supervised devices only.**
- Log out/delete user: **Available only with Shared iPad.**
- Enable/disable Lost Mode: **Available for supervised devices only.**
- Fetch device location: **Available for supervised devices only.**
- Rename device.
- Remote wipe: **Not supported on a Shared iPad.**
- Lock device.

- Push/remove settings.
- Push/remove apps and books.
- Request/stop AirPlay mirroring.
- Update information.
- Enroll/remove device.
- Install iOS update: **Requires the device be in Apple Deployment Programs (for business).**
- Update DEP profile: **Requires the device be in Apple Deployment Programs (for business).**

App Management

Windows 10 supports integration of Windows Store for Business subscriptions with MDM to deploy apps. To use an MDM system to deploy LOB apps directly to devices, a certificate authority must cryptographically sign all software packages. An enterprise can deploy a maximum of 20 self-signed LOB apps to a Windows 10 Mobile device, and more than 20 if the organization’s devices run Windows 10 Mobile Enterprise. Windows 10 WIP specifies which apps are allowed and disallowed and manages app classification without app wrapping or app modification. Admins do not need to add or remove classified apps from a device, including when wiping enterprise information. WIP does not tamper with existing personal apps and data. App restrictions also include use of Windows Store, private store, auto-updating, side loading, and multiple users on the same app to share data.

Apple offers a Volume Purchasing Program (VPP) through which organizations can purchase apps for end users. Employees still have to download the apps themselves using redemption codes provided by IT. With iOS 10, the VPP will let organizations buy apps and assign them to employees while retaining license ownership, which means employers can redeploy apps among users as staff turns over and job roles change.

iOS 10 defines MDM installed apps as managed apps. MDM specifies whether managed apps and their data remain on the device when the user unenrolls. It can prevent backing up of data from managed apps to iTunes or iCloud. iOS 10 also allows MDM to convert unmanaged apps to managed apps without reinstalling the app or losing user data. Supervised devices do not require user interaction for converting unmanaged apps to managed apps. Unsupervised devices require the user formally accept management.

MDM can remove managed apps from an iOS 10 device remotely or when a user removes the device. Removing an app also removes the data associated with it. If MDM removes a managed app but it remains assigned to the user, the user can download that app from the App Store as unmanaged. If MDM revokes an app license, it continues to function for a limited time. Eventually the app is disabled, and the user must purchase a copy to continue using it.

Remote Administration

MDM can query Windows 10 devices for hardware inventory, device name, username, email address, operating system and version, certificates, location, Wi-Fi MAC address, device ID, ownership designation, basic input/output system, screen resolution, OS language, and inventory of both Windows Store and non-Store apps.

MDM can query iOS 10 devices for a similar variety of information, including hardware serial number, device name, and Wi-Fi MAC address. It can also query for software information, such as device version and restrictions, and list the apps installed on the device.

Windows 10 introduces Windows 10 as a Service, a model for delivering OS feature updates more frequently than past Windows releases. In the past, new Windows releases happened every three years. This faster release pace is intended to address constantly evolving security threats along with meeting user expectations of new functionality on a regular basis. Microsoft plans to deliver updates two to three times per year, although it will release new capabilities on an ongoing basis. Windows 10 gets software updates directly from Windows Update, and for Windows 10 Mobile you cannot curate updates prior to deployment. Windows 10 Mobile Enterprise allows the enterprise to curate and validate updates prior to deploying them to the user population at large.

Apple does not publish a specific schedule for software or security updates but does generally deliver a major version update of iOS on an annual basis. Apple provides updates directly with no dependency on the mobile carriers. Apple has provided security updates at various times depending on the security flaw as a minor version update of the OS but, more commonly, Apple groups security updates together in major version updates of iOS. IT managers can put restrictions on devices that cannot be disabled by employees, such as forcing devices to allow automatic updates.

Windows 10 Mobile supports remote assistance to help resolve issues that users might encounter even when the help desk does not have physical access to the device. These features include remote lock, PIN reset, ring, and find. iOS 10 provides similar capabilities.

Diagnostics and Monitoring

Windows 10 provides audit information to track issues or perform remedial actions. This information provides assurance that device configuration complies with organizational standards. Windows 10 remote device health attestation uses measured boot data to verify the health status of the device. MDM leverages this health state, and correlated with client policies, to grant conditional access based on the current state of the device. The device must prove itself to be malware-free, have security tools active and fully updated to the correct patch level, or have access denied to designated resources. While iOS 10 does provide for querying of system information, it cannot provide conditional access based on device health information.

Microsoft routinely gathers Windows 10 telemetry, which is system data uploaded by the Connected User Experience and Telemetry component. This is primarily anonymous data used for OS diagnostics and improving the user experience. In order to disable this functionality on Windows 10 Mobile, customers must upgrade to the Windows 10 Mobile Enterprise edition. In Windows 10 Mobile Enterprise, the enterprise can configure telemetry at any of the four supported levels, including the security level. The Security level gathers only the telemetry info that is required to keep Windows devices secure with the latest security updates. To prevent Windows from sending any data to Microsoft, turn off Windows Defender telemetry and Malicious Software Removal Tool reporting, and turn off all other connections to Microsoft services.

Apple also has the ability to collect anonymous technical data used for improvement of products and services. This data is an opt-in process using the Diagnostic & Usage program to send nonidentifiable information about the device and applications. User explicit consent is required to do this, and the user can view the data on the device or stop sending data at any time.

Testing Scores

Management	Security Assurance Level (SAL)	Usability
Windows 10	93	93
iOS 10	81	81

For management, Windows 10 has a lower impact on usability for users and administrators. It supports the use of Azure Ad authentication for a single-step process of domain authentication, provisioning, and device management. iOS 10 supports SCEP for provisioning and domain accounts authentication to business apps. While effective, it is still not a single-step process with consistent user authentication. Windows 10 remote health attestation ensures device compliance from hardware to software, and conditional access limits exposure to devices that are not. iOS 10 does not provide similar remote health attestation, which limits its remote jailbreak detection capabilities. Microsoft also maintains a highly consistent security patch schedule, and Windows 10 has a method to provide security patches independent of OS updates; patch management is a critical process for organizational security.

Conclusions

After a comprehensive lab-based comparative feature assessment of the security and manageability capabilities of Windows 10 and iOS 10, it is Pique Solutions' conclusion that Windows 10 provides a better solution than iOS 10 for the enterprise.

Windows 10 provides cost-effective two-factor authentication for mobile devices, tablets, and PCs and eliminates the user password to mitigate the risk of compromise due to lost or stolen credentials. Windows 10 is the first OS to utilize FIDO 2.0 in an enterprise environment, and it supports multifactor authentication with asymmetrical keys in conjunction with hardware-based attestation to confirm the legitimacy of the keys. Windows Hello offers an extensible framework that enables the use of biometric sign-in options. The user's unique biometric identifier enables authenticated access to the device. While currently Windows Hello supports fingerprints, facial recognition, and iris scanning, new hardware may expand currently supported biometrics.

What's more, with WIP Windows 10 protects enterprise data in a way that is transparent to the user and allows a user to share a single app for both business and personal tasks. Windows 10 provides conditional access to enterprise resources based on device health attestation. Windows 10 leverages a unified OS architecture and app development platform across device types to streamline provisioning of devices and apps, including distribution of critical security updates and patches.

iOS 10 does provide incremental improvements over previous versions of iOS for enterprise environments. iOS 10 provides strong controls for a trusted chain of boot and signing apps, but it still requires third party integration for two-factor authentication and still lacks in functionality for managing and protecting enterprise data found in Windows 10.

Overall, Windows 10 consistently scored higher than iOS 10 in every measured category, particularly in identity management where Windows 10 can provide a unified authentication experience to the user and the enterprise. For data protection, Windows 10 applies encryption and controls to the data in such a way that proves to be both more effective and transparent to the user experience when compared to the managed app approach in iOS 10.

In terms of threat resistance, Windows 10 adds new capabilities for memory protection not yet seen in an OS. CFG provides a method for locking down and enforcing an app's flow of control once loaded into memory. Again, this is completely transparent to the user. For management capabilities, Windows 10 offers a diverse range of methods for managing the OS and a streamlined device provisioning and configuration process using domain accounts.

While both Windows 10 and iOS 10 provide comparable strong levels of encryption, we consider Windows 10 to be the superior implementation given the granular ability for encryption at the data level versus iOS 10's approach of applying encryption to the app. This is an element of Windows 10's ability to provide data protection at the data level using WIP. WIP's level of integration within the OS and enterprise apps also leads to a less intrusive user experience, where iOS 10 requires an app be designated personal or work with no dual-use capabilities.

Windows 10 also provides two distinct threat resistance features over iOS 10. The first is remote health attestation allowing for conditional access of a device to the trusted enterprise network dependent on the current device state including strong rooted device detection. Support for this type of conditional access based on remote health attestation is something not yet seen in iOS. The second is the introduction of new memory protection features that can limit an attacker's ability to compromise the system through memory attacks. Both of these features are transparent to the end user, except when a device is denied access to the network, in which case the user will be notified.

In short, Windows 10 can deliver resilient devices that meet the most stringent security and enterprise management requirements, while providing those controls in such way that is transparent to the end user and enhances rather than impedes productivity. What's more, it is Pique Solution's opinion that Windows 10 provides a more seamless device-wide experience for the administration and provisioning of devices by allowing the use of domain accounts as a single step for joining and configuring devices. For these reasons, we feel Windows 10 provides the better management experience and offers a unified software environment that should be considered by enterprise buyers.